UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,541	10/08/2001	Daniel R. Bolar	10010463-1	4434

29053 7590 08/04/2005

DALLAS OFFICE OF FULBRIGHT & JAWORSKI L.L.P.
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
MASKULINSKI, MICHAEL C	
ART UNIT	**PAPER NUMBER**
2113	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/972,541	**Applicant(s)** BOLAR, DANIEL R.	
	Examiner Michael C. Maskulinski	**Art Unit** 2113	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *18 and 26-29* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 19-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Non-Final Office Action

Claim Rejections - 35 USC § 102

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Claims 1-3, 7, 8, 11-13, 17, 20-22, and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Tentij et al., U.S. Patent 6,513,129.

Referring to claims 1, 11, and 20:

a. In Figure 1, Tentij et al. disclose network elements.

b. In column 1, lines 40-44, Tentij et al. disclose that the system includes a gateway and a management processor system. The gateway is communicatively connected to a network for receiving alarm incidents from the network (a gateway managing the network element and receiving fault alarm incidents from the network element).

c. In column 4, lines 43-47, Tentij et al. disclose management processors for handling policies relating to elements, the network, service, or business (distributed management servers communicatively associated with the gateway). Further, in column 5, lines 15-18, Tentij et al. disclose that basic control object processing is performed in the distributed gateways with advanced processing being performed in the management processor system (distributed management servers receiving control from said gateway to process said fault alarm incidents).

d. In column 4, lines 43-47, Tentij et al. disclose management processors for handling policies relating to elements, the network, service, or business. Further, in column 5, lines 28-34, Tentij et al. disclose that the management processor system may be implemented on one or more connected servers such that each processor may be physically distinct from the other (distributed management servers; and policy objects distributed across the distributed management servers so that each policy object resides on and is executable by a respective distributed management server).

e. In column 1, lines 41-47, Tentij et al. disclose that the gateway has a rule engine for selecting a control object from a set of control objects based on information from the alarm incident, and processing the selected control object. The management processor system has a processor for processing configuration objects in response to the selected control object for implementing fault management objectives defined by at least one user. Further, in column 4, lines 43-47, Tentij et al. disclose that identifying and parsing involves identifying the incident's source and associated management level so that it may be processed in the correct management processor (each policy object defining fault management behavior for managing the network element by the gateway, wherein a respective policy object is executed by the distributed management server on which the policy object resides in response to a respective fault alarm incident received by the gateway and associated with the policy object, to thereby implement the fault management behavior defined by the respective policy object in response to the respective fault alarm incident).

f. In column 1, lines 41-47, Tentij et al. disclose that the gateway has a rule engine for selecting a control object from a set of control objects based on information from the alarm incident, and processing the selected control object. The management processor system has a processor for processing configuration objects in response to the selected control object for implementing fault management objectives defined by at least one user. Further, in column 4, lines 43-47, Tentij et al. disclose that identifying and parsing involves identifying the incident's source and associated management level so that it may be processed in the correct management processor (wherein said gateway is capable of determining which said policy object corresponds to said fault alarm incident, said gateway is capable of selecting a distributed management server from said distributed management servers that is related to said policy object, said gateway capable of routing said fault alarm incident to said selected distributed management server. Further, in column 5, lines 15-18, Tentij et al. disclose that basic control object processing is performed in the distributed gateways with advanced processing being performed in the management processor system (said gateway capable of transferring control of processing said fault alarm incident according to said policy object to said selected distributed management server).

Referring to claims 2, 12, and 21, in column 4, lines 36-47, Tentij et al. disclose that the gateways include a rule engine for identifying and parsing incoming incidents that involves identifying the incident's source and associated management level so that it may be processed in the correct management processor (a decision object stored in the gateway, the decision object defining decision behavior for routing fault alarm incidents received by the gateway from the network element to an appropriate distributed management server for execution of a policy object residing on said appropriate distributed management server).

Referring to claims 3 and 13, in column 7, lines 44-56, Tentij et al. disclose that the gateway rule engine uses a combination of hierarchical and relational logic for selecting the "closest" control object. The incoming incident is matched, from very specifically to very generally, against a set of possible control object name strings. For example, an incident could include information about a network element including its domain, its function, and its specific assigned identification code. The rule engine would look for a control object name with all of these parameters; however, if not found, it could then select one with two or even just one of the parameters (the decision object is a data path tree associating attributes of the network element with a respective policy object).

Referring to claims 7, 17, and 25, in column 8, lines 35-39, Tentij et al. disclose that the management processing system would take appropriate action such as displaying alert information on the display terminal interface. In other cases, the basic processing in the gateway may directly cause an alert message to be displayed on the

Alert Display (an alert server generating alerts based on fault conditions in accordance with the policy objects).

Referring to claim 8, in column 6, lines 23-27, Tentij et al. disclose that the MIB (management information base) is an information base for storing objects and rules for managing the network tag in response to incoming incidents. In one embodiment, MIB comprises Network elements section, application rules section, and configuration objects section (a management information base operable to store software objects corresponding to the network element).

Referring to claim 22, in column 6, lines 23-27, Tentij et al. disclose that the MIB (management information base) is an information base for storing objects and rules for managing the network tag in response to incoming incidents. In one embodiment, MIB comprises Network elements section, application rules section, and configuration objects section (means for associating attributes of the managed network elements with the distributed management servers for implementing the fault management behaviors defined by the software).

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 4-6, 9, 10, 14-16, 19, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tentij et al., U.S. Patent 6,513,129 B1, and further in view of Fenger et al., U.S. Patent 6,751,659 B1.

Referring to claims 4 and 14, in column 6, lines 23-27, Tentij et al. disclose an MIB that is an information base for storing objects and rules for managing the network tag in response to incoming incidents. However, Tentij et al. don't explicitly disclose a policy server communicatively coupled to the distributed management servers, the policy server storing policy objects and operable to distribute the stored policy objects to the distributed management servers. In column 1, lines 60-65, Fenger et al. disclose that the primary server (policy server) maintains and manages a set of policy rules in a form of a policy tree. It would have been obvious to one of ordinary skill at the time of the invention to include the policy server of Fenger et al. into the system of Tentij et al. A person of ordinary skill in the art would have been motivated to make the modification because a central location for storing policy rules allows a user of the system to change a policy and have the changes reflected in all of sub-systems (see Fenger et al.: column 2, lines 30-40). This simplifies the process of making policy rule changes.

Referring to claims 5, 15, and 19, in column 7, lines 10-14, Tentij et al. disclose a configuration editor used for editing the configuration objects within the configuration objects section. Configuration objects are edited in order to change how incoming incidents are processed so as to effectuate the objectives or policies of the management system (a policy builder user interface communicatively coupled to the policy server, the policy builder user interface operable to receive input from a user for defining policy objects).

Referring to claims 6 and 16, in column 2, lines 57-67 continued in column 3, lines 1-8, Fenger et al. disclose that the target identifies itself, describes its capabilities and roles in the network, such as giving user ID or requesting certain resources, and describes how it is configured to work within the network. The policy server uses the information about the target as a filter to select the relevant subset of policy information for delivery to the target (a configuration file communicatively accessible by the policy server, the configuration file storing information defining the distributed management servers to which the policy objects are to reside).

Referring to claim 9, in column 7, lines 10-14, Tentij et al. disclose a configuration editor used for editing the configuration objects within the configuration objects section. Configuration objects are edited in order to change how incoming incidents are processed so as to effectuate the objectives or policies of the management system (a policy builder comprising an interface operable to receive user input defining said information stored to the configuration file).

Referring to claim 10, in column 2, lines 63-67 continued in column 3, lines 1-8, Fenger et al. disclose that the target identifies itself, describes its capabilities and roles in the network, such as giving user ID or requesting certain resources, and describes how it is configured to work within the network. The policy server uses the information about the target as a filter to select the relevant subset of policy information for delivery to the target (logic executable to distribute the policy objects to the distributed management servers in accordance with the configuration file).

Referring to claim 23, in column 6, lines 23-27, Tentij et al. disclose an MIB that is an information base for storing objects and rules for managing the network tag in response to incoming incidents. However, Tentij et al. don't explicitly disclose a means for distributing the software objects to the distributed management servers. In column 1, lines 60-65, Fenger et al. disclose that the primary server maintains and manages a set of policy rules in a form of a policy tree and distributes them accordingly. It would have been obvious to one of ordinary skill at the time of the invention to include the primary server of Fenger et al. into the system of Tentij et al. A person of ordinary skill in the art would have been motivated to make the modification because a central location for storing policy rules allows a user of the system to change a policy and have the changes reflected in all of sub-systems (see Fenger et al.: column 2, lines 30-40). This simplifies the process of making policy rule changes.

Referring to claim 24, in column 7, lines 10-14, Tentij et al. disclose a configuration editor used for editing the configuration objects within the configuration objects section. Configuration objects are edited in order to change how incoming incidents are processed so as to effectuate the objectives or policies of the management system (means for graphically generating the software objects).

Response to Arguments

5. Applicant's arguments filed June 24, 2005 have been fully considered but they are not persuasive.

6. On page 9, under section II (2), the Applicant argues, “Tentij teaches away from Applicant’s distributed management servers as claimed in amended claim 1.” The Examiner respectfully disagrees. In column 5, lines 15-18, Tentij et al. disclose that basic control object processing is performed in the distributed gateways with advanced processing being performed in the management processor system. Claim 1 states that

the distributed management servers receive control from said gateway to process said fault alarm incidents. This limitation doesn't state that the gateways can't perform processing before forwarding the fault alarm. Tentij et el. still teach forwarding the fault to a management processor.

7. On page 9, under section II (3), the Applicant argues, "Tentij discloses a 'rule engine' in the gateway that determines the 'closest' object (col. 8, lines 16-30). Applicant, on the other hand, claims (amended claim 1) that a gateway can determine which policy object corresponds to which fault alarm incident." The Examiner doesn't see the difference considering that the gateway of Tentij et al. is still capable of determining which policy object corresponds to which fault alarm incident. How Tentij et al. arrive at this conclusion is not important since the Applicant only claims that the gateway determines which policy object corresponds to which fault alarm incident and not how the gateway arrives at this conclusion.

8. On page 10, under section II (3) (a), the Applicant argues, "Applicant respectfully points out that Tentij states that the gateway processes the selected control object (col. 1, line 44), which is contrary to Applicant's amended claim 1 in which the gateway is capable of transferring control of processing the fault alarm incident according to the policy object to the selected distributed management server." The Examiner respectfully disagrees. This aspect of Tentij et al. is not contrary to the Applicant's invention because Tentij et al. still forwards the fault to management processors (see column 5, lines 15-18).

9. On page 10, under section II (3) (b), the Applicant argues, "Applicant respectfully points out that Tentij teaches away from Applicant's claimed policy objects distributed across distributed management servers because Tentij states that 'cross element manager or cross domain processing would typically not be carried out in the gateways' (col. 5, lines 18-20), and further, that 'the management processor system…perform basic, as well as advanced processing tasks, for managing or implementing a given function (e.g. fault,…) across various management layers' (col. 5, lines 23-28)." The Examiner respectfully disagrees. The section cited by the Applicant teaches that faults distributed across **gateways** would not include cross element manager or cross domain processing. However, faults can still be distributed across management processors.

10. On page 11, under section II (3) (c), the Applicant argues, "Applicant respectfully points out that Tentij states that a fault processing system is controlled by a gateway. On the contrary, Tentij does not disclose Applicant's claimed gateway that is capable of selecting a distributed management server, routing a fault alarm incident to the selected distributed management server, and transferring control of processing the fault alarm incident to the selected distributed management server, because Tentij does not disclose a transfer of control." The Examiner respectfully disagrees for at least the rejection above and the reasons given in paragraph 8.

11. On page 12, under section III, the Applicant argues, "Applicant respectfully asserts that Fenger teaches away from Applicant's claimed policy objects that define fault management behavior and that are distributed across distributed management servers so that each policy object resides on and executable by a respective distributed

management server (amended claim 11). On the contrary, Fenger states that policy rules are conditions for a user/application system to access a resource, and that not all of the policy rules need to be distributed to each and every component in the network (col. 1, lines 53-54). In the system of Fenger, rules are picked from the policy tree and distributed individually instead of Applicant's claimed defining policy objects (Applicant's claim 5)." The Examiner respectfully disagrees. The limitation of claim 11 does not state that each policy object exists on every management server but rather states that each policy object is on a respective management server. This is in line with what is taught by Fenger.

12. On page 13, under section III, the Applicant argues, "Applicant respectfully points out that the teachings of Tentij and Fenger together do not describe Applicant's claimed policy objects that are stored and distributed from a policy server (applicant's claim 4)." The Examiner respectfully disagrees for at least the reasons given in the rejection above.

13. On page 13, under section III, the Applicant argues, "Applicant respectfully points out that Tentij teaches an editor, but Tentij does not teach a user interface, as Applicant claims (claim 5)." The Examiner respectfully disagrees. The editor must have some kind of user interface, therefore, it is inherent. How could the editor be used without a user interface? The Examiner requests that the Applicant show how the editor is used without a user interface.

14. On page 13, under section III, the Applicant argues, "Applicant respectfully points out that nowhere does Fenger disclose policy objects, so that the combination of Fenger

with Tentij to meet the deficiencies of Tentij is not appropriate." The Examiner respectfully disagrees. The **entire** reference of Fenger et al. is concerned with policy information. The Examiner doesn't see how Fenger et al. couldn't possibly have policy objects. In the Abstract alone, Fenger et al. discuss a data structure, which is an object.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael C. Maskulinski whose telephone number is (571) 272-3649. The examiner can normally be reached on Monday-Friday 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MM